FDTC 2021: Final Program (PDF)

FDTC 2021 is a Virtual Conference (Zoom Webinar)

Schedule refers to Central European Summer Time (CEST)

Start: 09:15 CEST (03:15 am New York – 04:15 pm Tokyo)

09:15 – 09:30 Opening remarks

Keynote I

Chair: Luca Breveglieri

09:30 – 10:20 Managing Natural Hazards and Adversarial Fault Injections in the Context of Connected Emebedded Systems
Sylvain Guilley

10:20 – 10:50 Break

Session 1 – Fault Analysis

Chair: Shivam Bhasin

10:50 – 11:15 On the Importance of Initial Solutions Selection in Fault Injection
Marina Krček, Daniele Fronte and Stjepan Picek

11:15 – 11:40 A High-Order Infective Countermeasure Framework
Guillaume Barbu, Luk Bettale, Laurent Castelnovi, Thomas Chabrier, Nicolas Debande, Christophe Giraud and Nathan Reboud

11:40 – 12:05 ARCHIE: A QEMU-Based Framework for Architecture-Independent Evaluation of Faults
Florian Hauschild, Kathrin Garb, Lukas Auer, Bodo Selmke and Johannes Obermaier

12:05 – 12:30 EM Fault Model Characterization on SoCs: From Different Architectures to the Same Fault Model
Thomas Trouchkine, Guillaume Bouffard and Jessy Clédière

12:30 – 13:30 Lunch

Session 2 – Short Presentations

Chair: Guillaume Bouffard

13:30 – 13:45 Safe-Error Analysis of Post-Quantum Cryptography Algorithms
Luk Bettale, Simon Montoya and Guénaël Renault

13:45 – 14:00 Algebraic Fault Analysis of Subterranean 2.0
Michael Gruber, Patrick Karl and Georg Sigl

14:00 – 14:15 Are Cold Boot Attacks still Feasible: A Case Study on Raspberry Pi with Stacked Memory
Yoo-Seung Won and Shivam Bhasin

14:15 – 14:30 EMFI for Safety-Critical Testing of Automotive Systems
Colin O'Flynn

Keynote II

Chair: Luca Breveglieri

14:30 – 15:20 Fault Attacks against your Zen
Jean-Pierre Seifert

15:20 – 15:50 Break

Session 3 – Experimentation on Fault Attacks

Chair: Victor Lomné

15:50 – 16:15 On the Scaling of EMFI Probe
Julien Toulemont, Geoffrey Chance, Jean-Marc Galliere, Frederick Mailly, Pascal Nouet and Philippe Maurine

16:15 – 16:40 Laser Fault Injection in a 32-bit Microcontroller: from the Flash Interface to the Execution Pipeline
Vanthanh Khuat, Jean-Luc Danger and Jean-Max Dutertre

16:40 – 17:05 The Forgotten Threat of Voltage Glitching: A Case Study on Nvidia Tegra X2 SoCs
Otto Bittner, Thilo Krachenfels, Andreas Galauner and Jean-Pierre Seifert

Panel Discussion

Moderator: Sylvain Guilley

17:05 – 17:55 Electromagnetic Disturbance in the Industry
Arthur Beckers, Philippe Maurine, Colin O'Flynn and Stjepan Picek

New capabilities have emerged where electromagnetic (EM) benchs are used to cryptanalyze chips. The progress of this "research field" is fast, in terms of reproducibility, accuracy and number of use cases. Yet there is not enough awareness about such advances and their security threats. We discuss quantitative metrics to assess the harmfulness of EM fault injection (EMFI), so as to allow for a pre-silicon (source-code level) validation of the robustness against EMFI attacks and therefore for a reasonable security assessment.

17:55 – 18:00 Closing remarks and Farewell